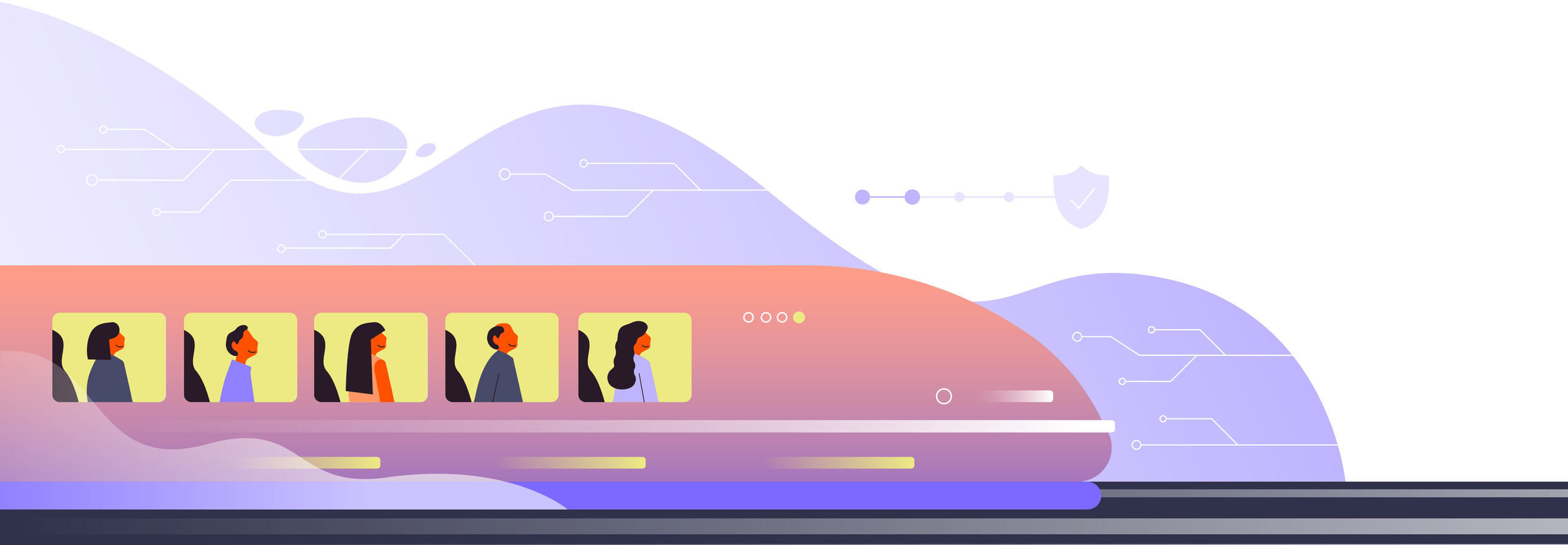
Security Room
infonet
solutions

Documento riservato

Cybersecurity is never a destination,
It’s a journey we’re on together!



Security Room Identity

Why us?

La Security Room di Infonet Solutions opera con **approccio olistico** nei confronti della sicurezza informatica. Integra soluzioni e servizi a tutto tondo eseguendo attività di analisi e consulenza continua rispetto ai gap di sicurezza identificati (**Security Review**), **aiutando le aziende ad avvalersi di infrastrutture di sicurezza implementate, configurate e gestite secondo una logica di *Security By Design*.**

Crediamo che un persorso volto al miglioramento della propria sicurezza lo si debba progettare e realizzare poco per volta, perseverando e prevedendo insieme eventuali cambi di rotta e nuovi orizzonti:

"Cybersecurity is never a destination, it's a journey we're on together!"

Il nostro approccio

Hack the Gap!

Spostare il focus dalla soluzione al problema, significa riconsiderare il modo di approcciare alla sicurezza informatica. Nella pratica, vuol dire determinare, in primis, le reali vulnerabilità esistenti, per poter vagliare successivamente le contromisure più efficaci da sviluppare.

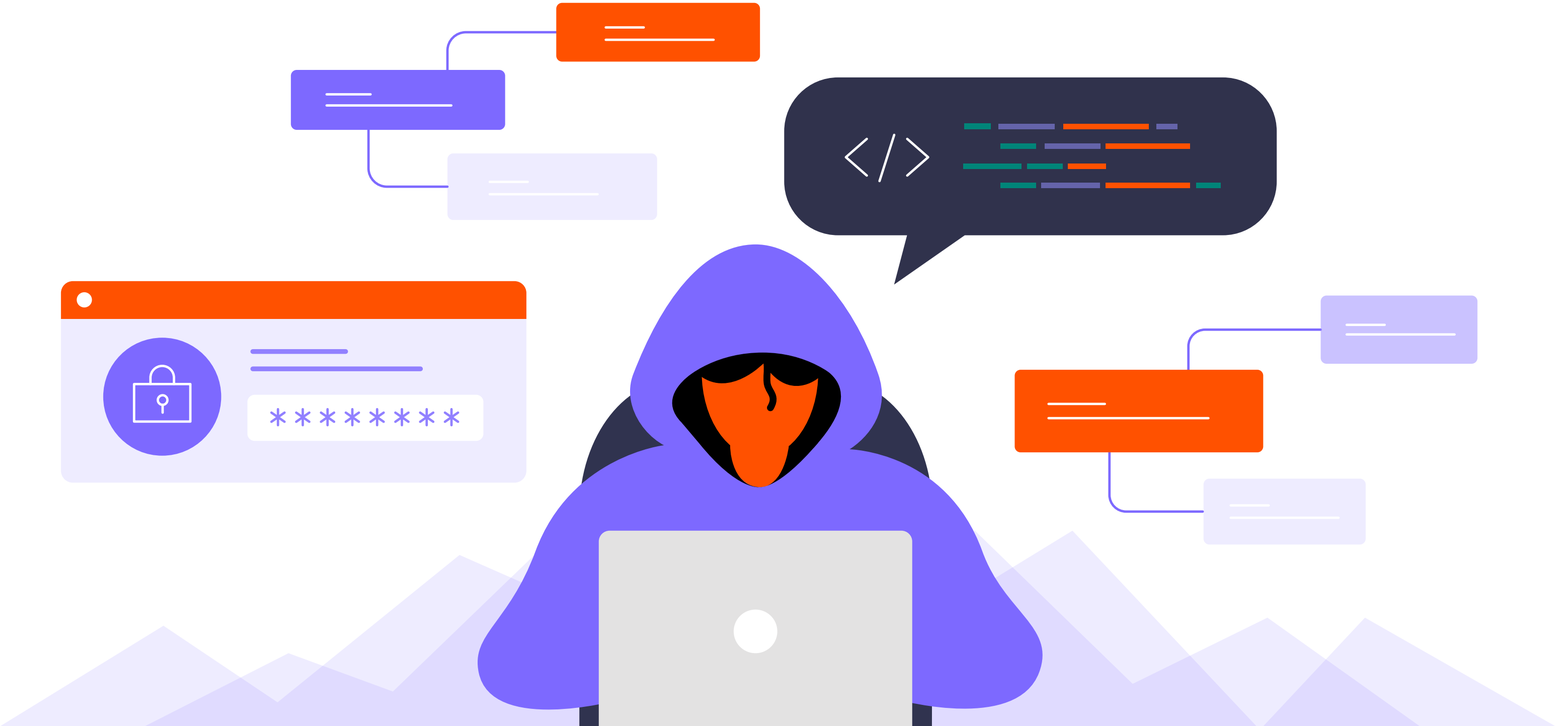
La Security Room di Infonet Solutions propone una suite di soluzioni e servizi di Cyber Security idonei a fronteggiare e proteggere i fattori e le vulnerabilità maggiormente sfruttate ad oggi dal cyber crime per entrare all'interno dei sistemi aziendali e muoversi indisturbati.

The Malicious Agent Path & The Most Efficient Solutions

Documento riservato

Il Maliciuos Agent Path mostra le principali fasi di un attacco informatico: dall'accesso iniziale, i movimenti e le eventuali escalation, fino ad arrivare all'esfiltrazione di dati o al blocco dei sistemi.

Per ognuna di queste tipologie di attacco, la nostra Security Room propone una serie di remediation e contromisure da mettere in atto, per bloccare e mitigare i rischi associati ad un eventuale attacco informatico.



Documento riservato

The Attack

Initial Access
- Fraud Prevention
- Phishing Assessment
- Security Training & Awareness
- Mobile Device Management
- Web Application Firewall

Discovery
- SIEM
- Network AI Defense
- IPS (Intrusion Prevention System)

Credential Access
- MFA
- Password Management
- Passwordless
- Biometrics
- Least Privilege

Exploitation
- Vulnerability Assessment
- Penetration Test
- Vulnerability Management

Privilege Escalation
- Remediation Plan
- Enforcement Active Directory & Azure AD
- OS Hardening

Defense Evasion
- Extended Detection & Response (XDR)
- Incident Response
- Application allow listing

Persistence
- Content Disarm Reconstruction
- EndPoint Security
- Network Security
- Virtual Patching

Lateral Movement
- Micro-segmentation
- SASE-Secure Access Service Edge
- Intrusion Prevention/Detection

Collection
- Data Access Governance
- Database Security
- Information Management
- Cloud Security

Command & Control
- Protective DNS
- Firewall
- Security Monitoring

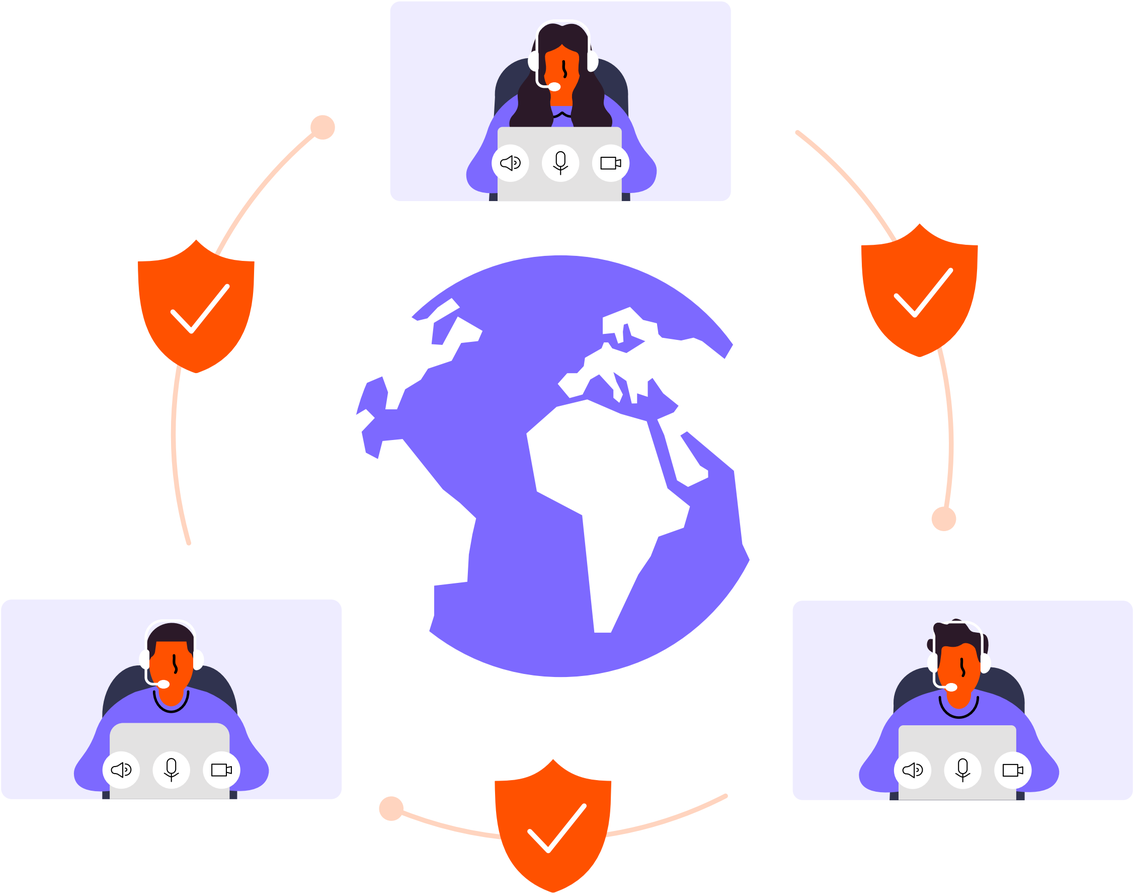
Exfiltration
- Data Loss Prevention
- Crittografia dati
- Backup
- Disaster Recovery
- IT Forensics

Managed Detection & Response

Hunt Threats Continuously

Documento riservato

Grazie al monitoraggio attivo h24, 7 giorni su 7, dei sistemi e del presidio costante di un team di **Analysts & Threat Hunters**, la Security Room di Infonet Solutions assicura l'analisi in tempo reale degli eventi. L'obiettivo è ridurre al minimo i falsi positivi e dare una risposta efficace ai cyber attacchi che minacciano piccole, medie e grandi imprese.



1 Managed SIEM

Con il supporto dell'intelligenza artificiale e di una tecnologia di machine learning (AI Cyber Defense), questo servizio è in grado di acquisire tutte le informazioni necessarie dai dispositivi IT aziendali (PC, server, apparati di rete, firewall, etc.) e di segnalare eventuali eventi di sicurezza.

Il servizio SIEM permette:

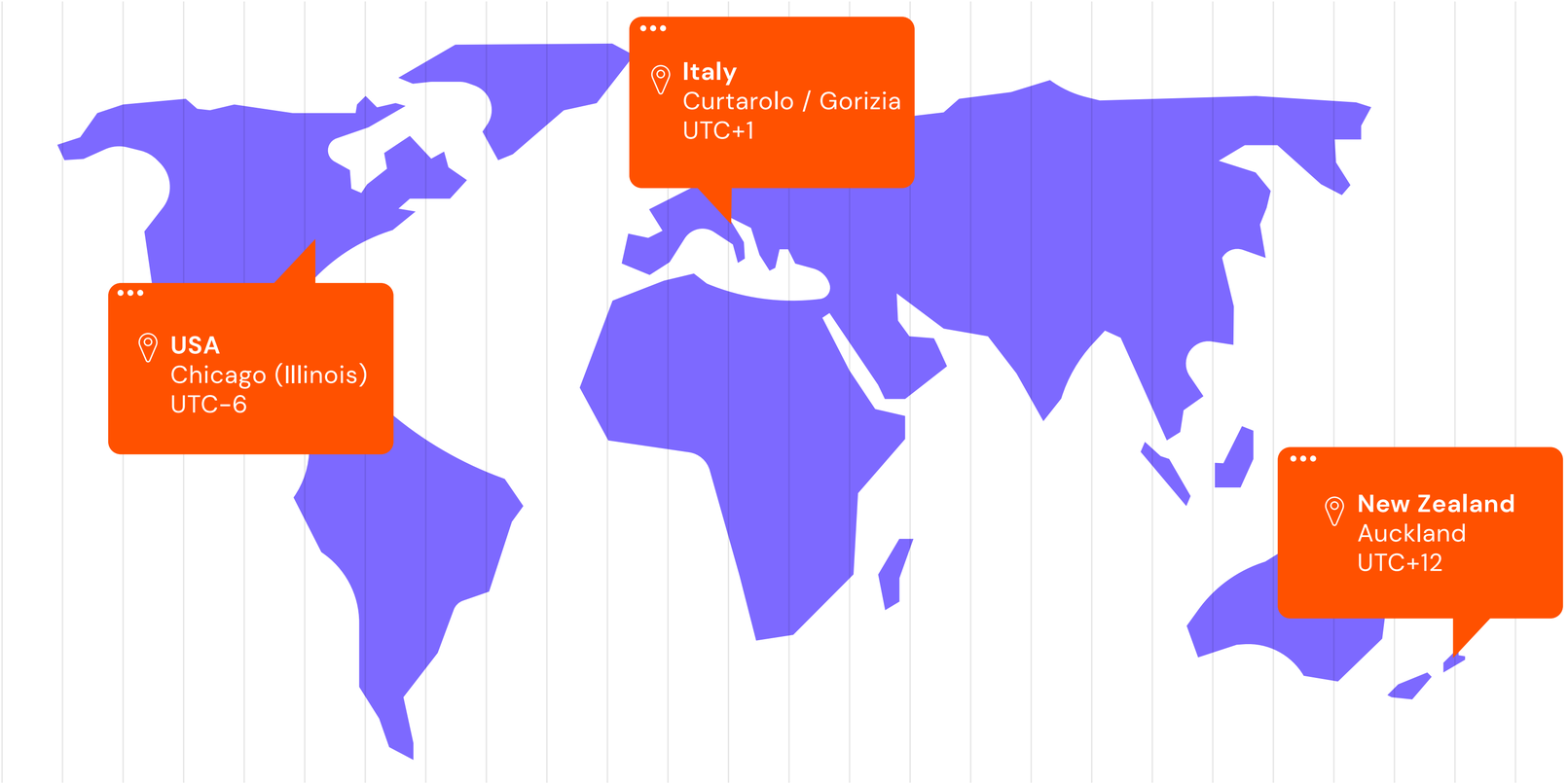
- **Controllo continuo delle Offense**: attività sospette rilevate dal SIEM in relazione alle regole e correlazioni definite.
- **Analisi e definizione delle Remediation** relative alle Offense che non sono state classificate come falsi positivi.
- **Revisione periodica delle regole di correlazione** allo scopo di mantenere in efficienza la soluzione e di adattarle agli scenari che mutano in base ai nuovi attacchi.
- **Mantenimento del sistema aggiornato** in base alle nuove feature di analisi dello strumento.

Il SIEM di Infonet Solutions ti garantisce di:

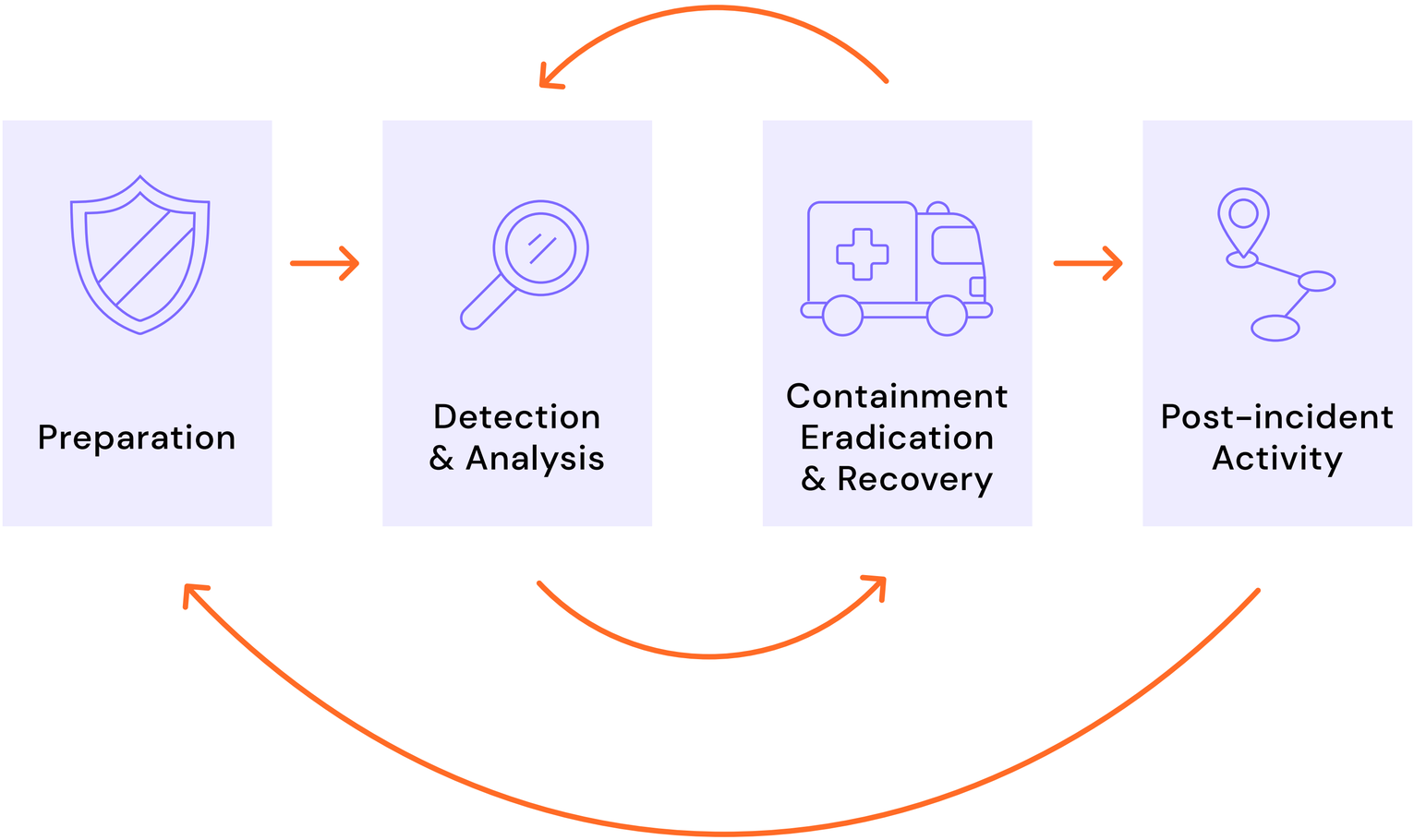
- Consolidare e **correlare gli inputs provenienti da più sistemi.**
- **Identificare gli incidenti** o i potenziali incidenti di sicurezza.
- **Notificarlo** al team IT dedicato.
- **Dare priorità** agli incidenti ritenuti più pericolosi e d'impatto sul proprio business.
- **Tracciare** gli incidenti fintanto non siano stati presi in carico e chiusi.
- Fornire il **monitoraggio sulla stato di salute** della sicurezza e notificare gli eventuali alert.
- **Integrarsi** con i principali sistemi di gestione IT.
- **Implementare** automaticamente delle **best practices** da seguire affinché gli strumenti monitorati dal SIEM assicurino un livello di sicurezza adeguato.
- **Intercettare eventuali deviazioni** rispetto alle linee di buona condotta definite.

2 Cybersecurity Analysts & Threat Hunters

Si tratta della parte umana del servizio di monitoraggio H24 della Security Room, preposta alla **gestione degli eventi di sicurezza**. Un servizio **H24** erogato da un **team di specialisti e analisti** che analizzano ed intercettano gli allarmi provenienti dalla rete aziendale. In caso di attacco, gli specialisti del team di Security attivano le procedure di risposta e di gestione dell'incidente, contattando l'azienda, fornendo supporto, mitigazione e miglioramento continuo delle soluzioni di sicurezza (**Security Review**).



Cyber Incident Response Cycle



Security Assessment

Gain Visibility & Resilience

Documento riservato

Servizio rivolto non solo a sistemi ed applicazioni, ma anche a dispositivi mobili, IoT, sistemi ICS/Scada e al fattore umano, permettendo all'azienda di **verificare il livello di sicurezza dei propri asset critici** e valutare il **livello di consapevolezza** dei propri utenti.

1 Vulnerability Assessment

Per aiutarti a identificare, classificare ed affrontare i maggiori rischi per la sicurezza del tuo ambiente IT, evitando che eventuali vulnerabilità non risolte, quali ad esempio errori di configurazione, bug di sistema, utenti con privilegi troppo elevati possano esporre l'azienda ed il business a gravi conseguenze. Si tratta di un vero e proprio scanning dei propri asset IT, utile ad adottare le opportune contromisure

2 Peneration Test

Sfruttando le vulnerabilità identificate, il servizio di Penetration Test di Infonet Solutions simula come e con quali tipologie di attacco un malintenzionato potrebbe accedere all'interno dei propri sistemi, validando e verificando l'efficacia dei controlli di sicurezza implementati. La sua finalità è quella di evitare che un malintenzionato o una insufficienza del sistema possa compromettere la propria sicurezza

3 Phishing Assessment

Gli utenti di un'azienda sono il veicolo maggiormente sfruttato per arrivare a dati ed informazioni aziendali, poiché è molto più facile e proficuo sfruttare le vulnerabilità del fattore umano che aggirare le tecnologie e le infrastrutture di sicurezza implementate. Infonet Solutions esegue delle campagna di Phishing mirate ad evidenziare il livello di consapevolezza aziendale e identificare il corretto progetto di formazione, accompagnando l'azienda in un percorso di miglioramento della propria resilienza interna

Security Posture Improvement

Enhance your defense

Documento riservato

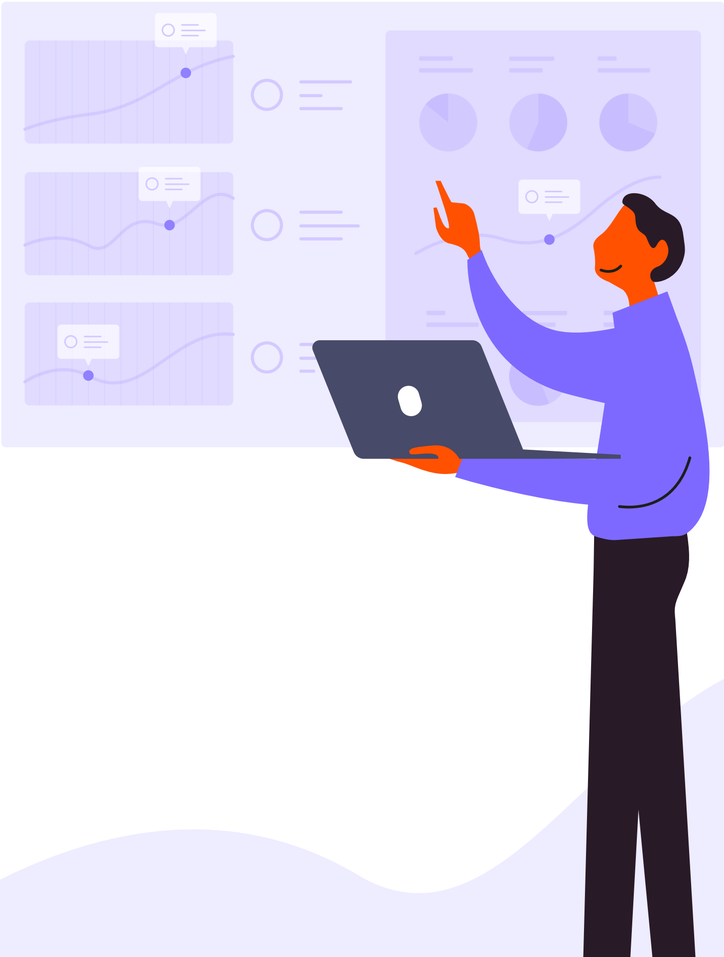
A fronte delle azioni di Assessment e di verifica delle reali vulnerabilità aziendali riscontrate, Infonet Solutions propone una serie di servizi e soluzioni dedicati a migliorare i propri gap di sicurezza.

La suite di soluzioni e servizi proposti considerano la protezione aziendale come un insieme di misure volte a migliorare l'aspetto **tecnologico**, **organizzativo** e **umano** della propria azienda.

1 Patching

Il servizio permette la completa gestione degli Endpoint (Client OS Microsoft, Mac, Linux, dispositivi Android e iOS) garantendo:

- **Gestione centralizzata delle patch**, sia del sistema operativo (Microsoft SCCM), sia del parco applicativo, sia di software di terze parti.
- **Gestione delle policy di sicurezza per l'utilizzo di USB e periferiche**.
- Distribuzione centralizzata dei sistemi operativi (**OS Deployment**) e delle applicazioni (Application Deployment).
- **Management remoto** per collegarsi ai clienti aziendali da un'unica interfaccia.
- **Vulnerability Manager**. Consente di tenere sotto controllo lo stato di installazione delle patch ed il livello di salute del proprio sistema (System Health), evidenziando i client più critici.
- **Software & Hardware Inventory**. Inventario IT su software ed hardware in uso.
- Integrazione con eventuali soluzioni di Service Desk.



2 Security Training & Awareness

La suite dei servizi dedicati a rendere i propri utenti più consapevoli delle attuali minacce informatiche, dando loro la capacità di saperle riconoscere e di reagire correttamente permettendo di:

- Ridurre le infezioni da malware e ransomware.
- Tutelare i dati aziendali da furti o accessi non autorizzati.
- Creare una corretta cultura sulla sicurezza delle informazioni.
- Tutelare il proprio business dalle minacce informatiche.

3 Active Directory Security Hardening

Servizio che ha lo scopo di individuare e descrivere un percorso che permetta l'adozione di una serie di configurazioni e tecnologie atte ad innalzare i livelli di sicurezza dell'ambiente Active Directory, del sistema di gestione delle identità e dei relativi livelli di permesso.

4 Firewall Management

Servizio che permette la gestione semplificata dei propri firewall, la corretta configurazione e gestione di un set di regole e di policy di sicurezza ed il controllo del traffico in entrata ed uscita nella propria rete.

5 Backup Management

Servizio ideato per le aziende che aspirano ad avere un partner che le aiuti nella corretta configurazione del proprio sistema di backup, nella gestione dell'intero processo di salvaguardia dei propri dati e del pronto ripristino in caso di anomalie.

Security Tool

Ad integrazione dei propri servizi di Cybersecurity, la Security Room di Infonet Solutions propone alcuni strumenti di **prevention** essenziali per migliorare problemi specifici e mitigare i rischi cyber associati agli utenti e all'utilizzo quotidiano della tecnologia.

Network Security

Soluzioni di protezione perimetrale, in particolar modo a difesa di e-mail e account aziendali (Network Access Control), protezione DNS e della navigazione web, protezione da attacchi di tipo DoS e DDoS.

Cloud Security

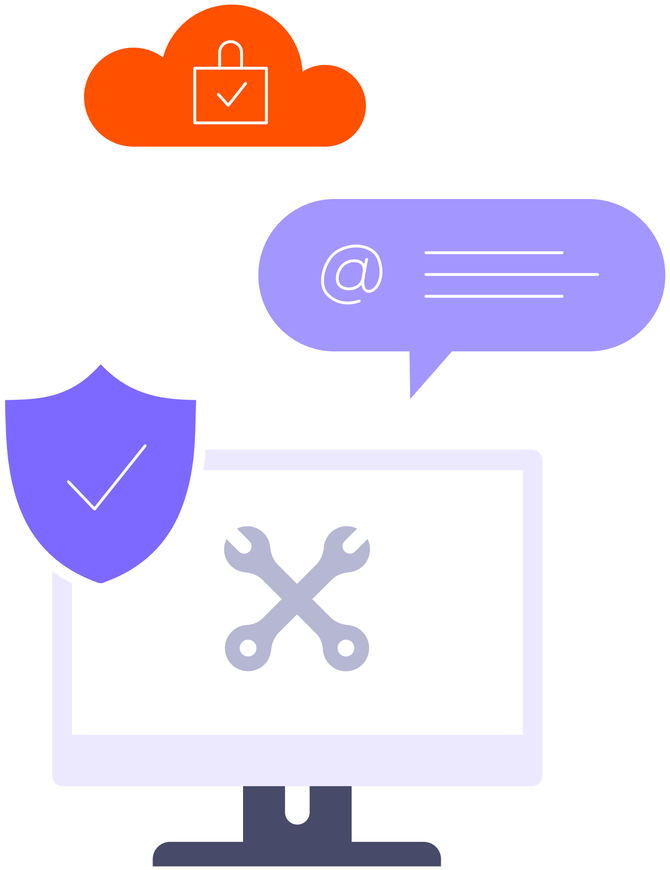
Soluzioni di protezione della propria architettura Cloud includendo soluzioni, tecnologie e procedure di controllo, quali ad esempio: micro-segmentazione dei data center, protezione, crittografia e conservazione dei dati, monitoraggio sul traffico, gestione e controllo delle identità tra le diverse piattaforme cloud utilizzate in azienda, corretta profilazione degli accessi e conformità legale.

Intrusion Prevention System (IPS)

Soluzioni di rilevamento di eventuali intrusioni e tentativi di attacco informatico attraverso l'analisi in tempo reale di anomalie relative al traffico (ad esempio carico elevato della CPU), tentativi di login insoliti, connessioni da indirizzi conosciuti, etc. Dati ed informazioni di sistema notificate in tempo reale per bloccare in modo proattivo tentativi di attacco informatico o accessi non autorizzati.

Deep Investigation & Fraud Prevention

Soluzione di Fraud Detection che offre alle aziende un'indagine preventiva nel Deep Web di eventuali password pubblicate, permettendo di avere visibilità dei propri dati rubati già nelle prime fasi del ciclo di vita delle violazioni e, di conseguenza, agire immediatamente per proteggere gli account aziendali compromessi e bloccare sul nascere la capacità dei criminali di poter accedere ai sistemi aziendali.



Security by Design

Progettazioni e configurazioni di architetture IT che integrano regole e procedure idonee ad innalzare i livelli di sicurezza informatica, anticipando potenziali debolezze e modalità di attacco informatico. Si tratta principalmente di soluzioni che, prevedendo l'inserimento di una serie di controlli e verifiche, consentono di ridurre a priori determinati rischi informatici associati sia agli utenti che all'aspetto progettuale ed implementativo dei sistemi aziendali.

Password Management

Strumenti per la corretta gestione, protezione e archiviazione di credenziali e password, evitando così i più comuni errori, quali: annotare password, utilizzare la stessa password per più account, scegliere password deboli e non aggiornate periodicamente.

Identity Management

Soluzioni e prodotti di passwordless e autenticazione biometrica consentono di agevolare gli utenti nell'accesso a servizi ed applicazioni aziendali evitando di dover conservare e memorizzare password in modo errato, esponendo l'azienda ad accessi non autorizzati all'interno dei propri sistemi.

Mobile Device Management (MDM)

Soluzioni che oltre a consentire la gestione dell'inventario ed il provisioning dei dispositivi, permettono di proteggere le applicazioni aziendali e i dati in essi contenuti. Questi strumenti garantiscono la protezione dei mobile e degli utenti da malware e da eventuali attacchi ad essi rivolti, potendo garantire la salvaguardia dei dati, la loro automatica cancellazione ed il loro ripristino in caso di attacco o furto.

Crittografia dei dati

Integrazione di soluzioni (hardware o software) di crittografia per la cifratura dei dati su server, chiavi USB, dischi o storage con sistema di cifratura integrati, dispositivi mobili, e-mail, browser e firme digitali.

Microsegmentazione

Applicando i principi dello Zero Trust, la soluzioni di microsegmentazione consentono la segmentazione delle reti e l'isolamento di applicazioni, separando le aree del network esposte ad Internet e quelle che invece contengono traffico molto più sensibile, evitando in caso di attacco informatico il movimento laterale di un agente malevolo e la conseguente compromissione, senza controllo, dell'intera rete aziendale.

infonet solutions

Sede Legale

Via Einaudi 23
ZI Pieve di Curtarolo (PD)
tel +39 049 9620572
fax +39 049 9620557
www.infonetsolutions.it

Headquarters

Via Garibaldi 3
35010 Curtarolo, Padova
tel +39 049 9620572
www.infonetsolutions.it

infonet 365

Via Trieste, 205
34079 Staranzano (GO)

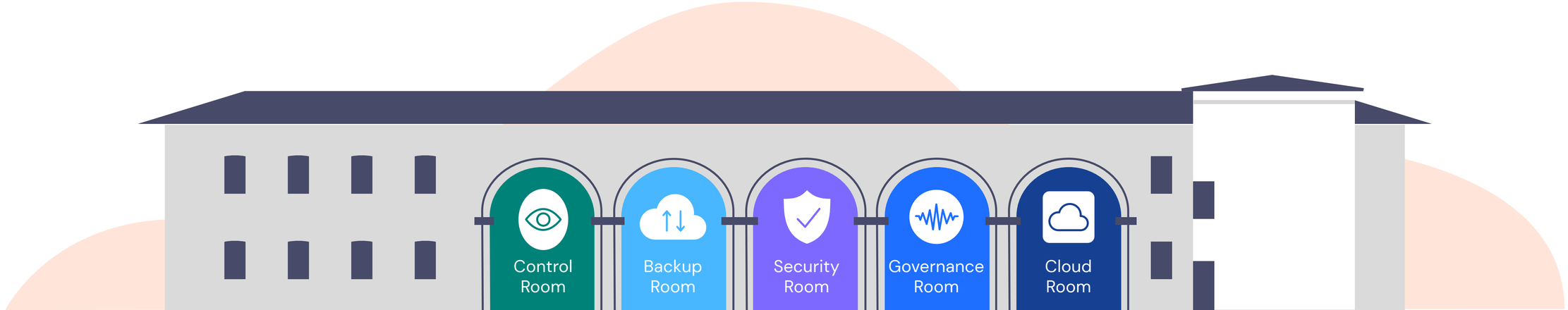
www.infonet365.it

infonet solutions OF ILLINOIS LLC

4320 Winfield Road – Suite200
Warrenville IL, 60555

www.infonetsolutionsgroup.us

Infonet Solutions NZ
Business Innovation

44 – 46 Constellation Drive
Rosedale, Auckland, 0632

www.infonetsolutions.co.nz